Requisitos de red NEO+ y NEXO

Ref: D-0028084-ES-r3

Handbook

Contenido

1 INTRODUCCIÓN 1

2 ARQUITECTURA DE RED 1

3 ESPECIFICACIONES DE RED. 1

3.1 Configuración ETX NEO+ 2

3.2 Configuración y requisitos VLANs FlexNet 2

4 Descripción del tráfico ACSINet, AES67 y FlexNet+ 2

4.1 Trafico audio IP/AES67 2

4.1.1 Protocolo de red IGMP 2

4.1.2 Protocolos e IPs 3

4.2 Trafico de Control 3

4.2.1 Ancho de banda 3

5 Configuración de Seguridad en redes. Buenas prácticas 4

5.1 Control de acceso físico 4

5.2 Funciones de Seguridad en Redes Multiservicio 4

1 INTRODUCCIÓN

Este documento detalla la especificación de red para la interconexión de sistemas de megafonía y evacuación de LDA Audio Tech, específicamente para las familias NEO+ y NEXO, así como para los accesorios que suelen integrarse con estos sistemas.

2 ARQUITECTURA DE RED

La arquitectura de red se divide en tres partes principales:

1. **Anillo redundante** del sistema de evacuación EN54-16. Zona dedicada a la interconexión de unidades NEO+ y NEXO mediante infraestructura de red dedicada formada por las conexiones de los propios equipos. En los sistemas distribuidos donde se necesita un enlace a mayor distancia, se dispone de un modelo homologado de conversor de medios que permite convertir el cable ethernet a fibra óptica.

2. **Red EN54** de interconexión entre sistemas. Los sistemas NEO+ pueden interconectarse entre sí formando un sistema mayor que puede ser gestionado desde uno o varios puntos de control general, a este tipo de sistemas los llamamos sistemas multi-site. La red que une sistemas NEO+ con micrófonos de evacuación se debe realizar con switches que hayan sido homologados para el sistema EN54. El sistema NEO+ de LDA Audio Tech incluye en su certificado un switch ethernet con alimentación redundante.

3. **Red multiservicio** auxiliar. Para el resto de los dispositivos del sistema de megafonía entre los que se incluyen micrófonos PA, reproductores de audio, equipos AES67 o Dante y otros dispositivos anexos al sistema.

3 ESPECIFICACIONES DE RED.

Los equipos del sistema NEO+ funcionan ahora con una configuración de red simplificada basada en una única VLAN compartida para el tráfico IP de audio y control. Esta configuración permite mayor flexibilidad en redes L3 y mejora la interoperabilidad con sistemas modernos. La gestión de ancho de banda y seguridad se hace mediante segmentación por dirección IP.

NOTA: En versiones anteriores del sistema NEO, los sistemas operaban bajo el esquema FlexNet de dos VLANs, usando una para control (VLAN 1) y otra para audio (VLAN 2) integradas en la red mediante puertos en modo trunk. Esta configuración sigue siendo compatible con NEO+ pero se considera obsoleta y no se puede usar en sistemas que integren NEXO o NEXO HUB fuera del anillo redundante.

3.1 Configuración ETX NEO+

Los puertos X del módulo ETX pueden ser configurados en:

- Modo trunk (Flexnet), todo el tráfico de audio y control sale por el puerto con formato tagged para su conexión a switches.
- Modo untagged, el tráfico sale sin Tag para ser accesible desde cualquier PC.
- Cuando se usa una única VLAN el tráfico de audio y control es accesible en los modos 01 y 10 del módulo ETX.
  En ambos casos la velocidad es de 100Mbits/s.

3.2 Configuración y requisitos VLANs FlexNet

El tipo de tráfico generado por los equipos se detalla en las secciones siguientes. El requisito general del tráfico del **anillo flexnet** es que la comunicación sobre esta VLANs sea **transparente**, permitiendo la comunicación **broadcast y multicast Ethernet L2** entre sus extremos sea cual sea el protocolo. De esta forma los equipos NEO y NEXO del anillo se comunican correctamente con 1 o 2 VLANs configuradas.

Existen diferentes protocolos en la infraestructura de red para hacer extender VLANs en grandes redes IP. Se podrán utilizar sistemas de enrutamiento tipo MPLS o similar dependiendo de la topología de la red multiservicio empleada.

4 Descripción del tráfico ACSINet, AES67 y FlexNet+

4.1 Trafico audio IP/AES67

Los paquetes de audio tienen como especial requisito la baja latencia que deben cumplir para funcionar correctamente y se envía un paquete de audio cada 1 ms.

El protocolo compatible con **AES67** se usa en los equipos NEO+, NEXO, EVACCore.

El tráfico que se utiliza es de tipo multicast IP que se dirige a los dispositivos receptores utilizando la gestión inteligente de la red.

4.1.1 Protocolo de red IGMP

Se usa para la coordinación de tráfico multicast a través de la red. Los equipos que quieren recibir un tráfico se subscriben y de esa forma el ancho de banda sólo se utiliza en los tramos donde hay receptores inscritos. Es fundamental tener correctamente configurada la red para este propósito.

Para conectar secciones de Redes a través de routers Layer 3 se necesitará activar el protocolo **PIM** entre ellos, para que las subscripciones **IGMP** puedan hacer llegar el tráfico a equipos conectados en los extremos de la red.

QoS y DSCP

El tráfico se prioriza en función de sus necesidades de latencia marcando el campo **DSCP** y activando el **QoS** en la red. El tráfico AES67 de LDA utiliza el valor 46 para audio (alta prioridad) y DSCP 56 para PTP(sincronización crítica).

4.1.2 Protocolos e IPs

PTPv2 para la sincronización de precisión de los dispositivos a valores de nanosegundos de diferencia. Por defecto usa la IP 224.0.1.129

Discover v3 de LDA AudioTech. Utiliza una dirección IP multicast registrada en IANA (224.0.2.11), a la que todos los dispositivos LDA se suscriben mediante IGMP y de esta forma facilitar la configuración de IPs sin necesidad de DHCP.

Audio IP. El audio se envía siguiendo el estándar AES67 que utiliza paquetes IP multicast para transmitir hasta 8 canales de audio. En la configuración estándar, cada transmisor de audio envía un paquete cada 1 milisegundo. Las direcciones IP se configuran manualmente o se eligen de la lista preconfigurada en los equipos.

El rango de direcciones es de 239.0.0.0 a 239.255.255.255. El documento "ACSINet multicast IP Addressing" especifica las direcciones IP usadas.

4.2 Trafico de Control

Los datos de control utilizan encapsulado IP con protocolo UDP principalmente. Dependiendo del tipo de comunicaciones se utilizará direccionamiento **unicast**, **multicast** o broadcast (sólo Discover v1), por lo que se debe dejar habilitado este tipo de tráfico dentro de la red local virtual.

Para la coordinación de equipos NEXO en Domains o NEXO HUB en Cluster se utilizan los mismos protocolos que en el audio, de forma que la configuración de red es exactamente la misma para ambos tráficos. En este caso las direcciones IP son específicas para control.

El tráfico incluye mecanismos de autenticación que deberían evitar cualquier tipo de problema de interferencia entre equipos o intrusión. En cualquier caso, la normativa anti-incendios obliga a proveer de un control de acceso físico a los dispositivos y puertos de comunicación.

4.2.1 Ancho de banda

- *VLAN de audio: Máximo ancho de banda utilizable 100Mbit/s*
  - *Cada Stream de 8 canales necesita 12Mbits/s aproximadamente*
- *VLAN de control. Máximo ancho de banda 1 Mbit/s*

Tamaño de paquetes. MTU

> *El tamaño máximo que puede contener el paquete de datos (MTU) estará por debajo de los 1.500 bytes.*

5 Configuración de Seguridad en redes. Buenas prácticas

Los sistemas de evacuación por voz se basan en la familia de normativas europeas EN54 para sistemas anti-incendio. Estos productos se integran dentro de la directiva de productos para la construcción, por lo que se requiere que sean certificados bajo estándares más exigentes que cualquier dispositivo de infraestructura de red o multimedia de propósito general.

La infraestructura del edificio y los puertos de conexión al sistema EN54 deben estar provistos de medidas de seguridad que impidan el acceso tanto físico como digital.

5.1 Control de acceso físico

El método más seguro es diseñar una red independiente con imposibilidad de acceso físico a ningún punto terminal de cableado donde se pueda acceder al sistema mediante conexión Ethernet IP.

5.2 Funciones de Seguridad en Redes Multiservicio

La infraestructura de red incluye medidas adicionales de control que se utilizan para impedir el acceso indeseado a los sistemas, algunas de estas medidas se listan a continuación. Se incluyen observaciones en relación a las necesidades o conflictos que puedan generar con los sistemas NEO+ y NEXO Hub.

1. **Privacidad VLAN**: Dividir una red en VLANs y en sub-VLANs para segmentar y aislar el tráfico entre dispositivos y sistemas que la conformen. Ayuda a limitar la comunicación directa entre dispositivos en la misma red, mejorando la seguridad.
    - Es un método de aislamiento esencial para controlar los puntos de acceso al sistema de evacuación.
    - Este documento detalla la separación en VLAN necesaria para el sistema.
2. **Control de Acceso** basado en MAC (PortSecurity): Permiten definir reglas para controlar el tráfico de red basado en las direcciones MAC que se conectan a cada puerto.
    - Cada equipo NEO+ tiene 2 direcciones MACs.
    - Cada equipo NEXO tiene 1 dirección MAC.
    - Un sistema NEO+ incluye un loop interno que puede superar las 100 direcciones MACs en el mismo puerto de la red multiservicio, además el equipo NEO+ backup comunicará estas mismas direcciones MAC en caso de entrar en funcionamiento.
    - Pueden existir conflictos con el sistema automático de detección de MACs. En caso de definir manualmente las direcciones permitidas debe existir un protocolo de coordinación para los casos donde se realice la sustitución de un equipo del sistema. Por esto se recomienda el uso del modo de notificación en lugar de bloqueo ante cambios de direcciones MACs.
    - El ámbito de actuación de este protocolo sólo tiene sentido en los lugares acceso público sin protección física.
3. **DHCP Snooping**: Previene ataques de DHCP mediante el monitoreo de mensajes DHCP y permitiendo solo aquellos de servidores DHCP autorizados. Evita que dispositivos no autorizados actúen como servidores DHCP.

4. **IP Source Guard**: Utiliza la información del DHCP Snooping para asegurarse de que las direcciones IP en los puertos coincidan con las direcciones MAC autorizadas, previniendo ataques de spoofing.
    - Sólo podría generar conflicto en caso de sustitución de equipos.
5. Dynamic ARP Inspection (DAI): Verifica los paquetes ARP para asegurarse de que contengan información válida, evitando ataques de ARP spoofing.
    - Ok, ningún conflicto
6. **Storm Control**: Protege contra tormentas de broadcast, multicast, y unicast al limitar la cantidad de tráfico que puede atravesar el switch. Ayuda a prevenir la congestión de la red causada por ataques o configuraciones incorrectas.
    - Tener en cuenta que los sistemas de audio digital transfieren mucho tráfico multicast y debe estar permitido. También se transmite tráfico broadcast entre los equipos del sistema.
7. Access Control Lists: Filtran el tráfico basado en varias capas del modelo OSI (por ejemplo, IP, protocolo, puertos TCP/UDP). Pueden ser configuradas para permitir o denegar tráfico específico, aumentando la seguridad.
    - Cuidado con los filtros de protocolos que puedan afectar. Ver las especificaciones de tráfico en este documento para más detalle. La recomendación es no activar filtros dentro de las VLANs del sistema de evacuación.

Protocolos catalogados como inseguros:

Existen listados de protocolos que se consideran inseguros actualmente, por ejemplo, FTP, telnet, TFTP, SNMP. LDA Audio Tech no usa ninguno de estos protocolos, pero sí que son ampliamente utilizados en múltiples sistemas industriales, por lo que la recomendación para estos casos es separar las redes de forma que el tráfico de los puntos accesibles no pueda nunca ser mezclado con los dispositivos sensibles.

Conflictos más probables con redes multiservicio:

Port Security, DDos filtering y LLDP: Cada equipo con módulo ETX integra dos direcciones MAC diferentes y un sistema NEO completo puede integrar hasta cientos de direcciones MAC a través de su puerto X. El tráfico generado desde cada una de estas direcciones MAC será cambiante en el tiempo dependiendo del uso del sistema y de sus procedimientos internos a nivel de monitorización, configuración, etc. Por esto se recomienda desactivar estos protocolos en esos puertos de la red multiservicio ya que pueden detectar como indeseable este tráfico. Es recomendable incluir una contramedida de seguridad equivalente como el control mediante protección física de los puertos accesibles por el público general.